

Serial No. 10/022,578

2

ONET-0101 PUS

In the Claims:

1. (Previously Presented) A method of authenticating a user having a user privilege server proxy for a network system having a privilege server, a head end server and a web adapter comprising:

presenting user information to the web adapter from the user privilege server proxy;

presenting the user information to the head end server;

presenting the user information to the privilege server from the head end server;

validating the user in response to the user information;

when a user is validated, generating a ticket for the user at the privilege server;

providing the ticket to the user privilege server proxy through the head end server;

forming a service access request token from the ticket and the user information;

sending the token from the user to the privilege server;

validating the user in response to the token;

forming a packet having a sequence number, session key and the ticket at the privilege server;

providing the packet to the head-end server;

in response to receiving the packet, authenticating the user at the head end server;

providing the packet to the user privilege server proxy;

sending the ticket and sequence number encrypted with the session key to a service server through the web adapter;

validating the user at the service server; and

granting the user role based privileges at the service server.

Serial No. 10/022,578

3

ONET-0101 PUS

2. (Previously Presented) A method as recited in claim 1 further comprising the step of negotiating an authentication scheme between the server proxy and privilege server.

3. (Previously Presented) A method as recited in claim 2 wherein negotiating the authentication scheme between the user privilege server proxy and privilege server comprises presenting at least one security mechanism from the user privilege server proxy to the privilege server; accepting or rejecting the at least one security mechanism at the privilege server.

4. (Previously Presented) A method as recited in claim 2 wherein the step of validating the user in response to the user information comprises validating the user in response to the user information in accordance with the authentication scheme.

5. (Original) A method as recited in claim 1 further comprising the step of encrypting the ticket with a user password to form an encrypted ticket.

6. (Previously Presented) A method as recited in claim 5 further comprising the step of decrypting the encrypted ticket at the user privilege server proxy.

7. (Previously Presented) A method as recited in claim 1 further comprising the steps of forming a packet having a sequence number and session key encrypted with the ticket at the privilege server and decrypting the packet at the user privilege server proxy.

8. (Currently Amended) A method of authenticating a user having a user privilege server proxy for a network system having a privilege server, a head end server and a web adapter comprising:

Serial No. 10/022,578

4

ONET-0101 PUS

negotiating an authentication scheme between the user privilege server proxy and the privilege server;

presenting user information to the web adapter;

presenting the user information to the head end server;

presenting the user information to the privilege server from the head end server;

validating the user at the privilege server in response to the user information in accordance with the authentication scheme;

when a user is validated, generating a ticket for the user at the privilege server;

encrypting the ticket with a user password to form an encrypted ticket;

providing the encrypted ticket to the user privilege server proxy through the head end server;

decrypting the encrypted ticket to form a decrypted ticket;

forming a service access request token from the decrypted ticket and the user identification information at the user privilege server proxy;

sending the token from the user privilege server proxy to the privilege server;

validating the user in response to the token;

forming a packet having a sequence number and session key encrypted with the ticket at the privilege server;

providing the packet to the head-end server;

in response to the packet, authenticating the user at the head end server;

providing the packet to the user privilege server proxy;

decrypting the packet;

sending the ticket and sequence number encrypted with the session key to a service server through the web adapter;

validating the user at the service server; and

Serial No. 10/022,578

5

ONET-0101 PUS

granting the user role based privileges at the service server.

9. (Previously Presented) A method as recited in claim 8 wherein negotiating an authentication scheme between the server proxy and privilege server comprises presenting at least one security mechanism from the user privilege server proxy to the privilege server and accepting or rejecting the at least one security mechanism at the privilege server.

10. (Currently Amended) A method as recited in claim 8 ~~comprising wherein the step of authenticating the user is performed~~ by a policy engine within the privilege server.

11. (Canceled)

12. (Currently Amended) A method for accessing a service by a user comprising:

presenting a user ticket and sequence number to a service through a web adapter;

choosing a service in ~~[[the]]~~ a service server;

sending ~~[[the]]~~ a session name encrypted with the ticket and a user identification to ~~[[the]]~~ a privilege server and requesting a session key and sequence number;

receiving the session name from the user;

validating the user ticket and a user privilege;

when the user is validated, issuing the session key and sequence number for the ticket;

encrypting the session key and sequence number with the ticket to ~~from~~ form a packet; and

sending the packet and ticket to the service.

Serial No. 10/022,578

6

ONET-0101 PUS

13. (Currently Amended) A system for authenticating a user having a user privilege server proxy for generating user information comprising:

a web adapter coupled to said user privilege server proxy for receiving user information;

a service server coupled to said web adapter;

an intermediate server coupled to the web adapter for receiving said user information; and

a privilege server coupled to said intermediate server, said privilege server receiving said user information and validating said user in response to said ~~[[use]]~~user information, said privilege server generating a ticket;

said user privilege server proxy receiving said ticket through said intermediate server, generating a token and communicating the token to the privilege server;

said privilege server generating a packet having a sequence number and a session key in response to said token and coupling said packet to said user privilege server proxy;

said user privilege server proxy coupling the ticket and the sequence number to ~~said~~a service server through said web adapter;

said service server validating said user and granting said user privileges in response to the ticket and the session key.

14. (Original) A system as recited in claim 13 wherein said intermediate server comprises a head end server.

15. (Original) A system as recited in claim 13 wherein said user information comprises a user identification number.

16. (Original) A system as recited in claim 13 wherein said privilege server has a policy engine therein.

Serial No. 10/022,578

7

ONET-0101 PUS

17. (Original) A system as recited in claim 16 wherein said privilege server comprises a key generator coupled to the policy engine.

18. (Original) A system as recited in claim 16 wherein said privilege server comprises a proxy coordinator coupled to the policy engine.

19. (Original) A system as recited in claim 16 wherein said privilege server comprises an obfuscator/deobfuscator coupled to the policy engine.

20. (Original) A system as recited in claim 16 wherein said privilege server comprises a store keeper coupled to the policy engine.

21. (Original) A system as recited in claim 20 wherein said store keeper comprises a user information list and a session information list.

22. (Original) A system as recited in claim 13 wherein said service server validating said user and granting said user privileges in response to the ticket, session key and sequence number.

23. (Currently Amended) A method of authenticating a user having a user privilege server proxy for a network system having a privilege server, a head end server and a web adapter, said method comprising:

determining an authentication scheme at the privilege server;

validating the user at the privilege server in response to user information in accordance with the authentication scheme;

when ~~[[a]]~~the user is validated, generating a ticket for the user at the privilege server;

encrypting the ticket with a user password to form an encrypted ticket;

Serial No. 10/022,578

8

ONET-0101 PUS

validating the user in response to a service access request token formed from the ticket and a user identification; and

forming a packet having a sequence number and session key encrypted with the ticket at the privilege server to authenticate the user.

24. (New) A method as in claim 1 wherein generating a ticket comprises generating a ticket with at least one of a session name and the user information.